Westinghouse Electric Company
Nuclear Power Plants
P.O. Box 355
Pittsburgh, Pennsylvania 15230-0355
USA

U.S. Nuclear Regulatory Commission
ATTENTION: Document Control Desk
Washington, D.C. 20555

Direct tel: 43-374-6206
Direct fax: 724-940-8505
e-mail: sisk1rb@westinghouse.com

Your ref: Docket No. 52-006
Our ref: DCP_NRC_002740

January 15, 2010

Subject: AP1000 Response to Proposed Open Item (Chapter 7)

Westinghouse is submitting the following responses to the NRC open item (OI) on Chapter 7. These proposed open item response are submitted in support of the AP1000 Design Certification Amendment Application (Docket No. 52-006). The information included in these responses is generic and is expected to apply to all COL applications referencing the AP1000 Design Certification and the AP1000 Design Certification Amendment Application.

Enclosure 1 provides the response for the following proposed Open Item(s):

OI-SRP7.1-ICE-02	OI-SRP7.2-ICE-04	OI-SRP7.9-ICE-02
OI-SRP7.1-ICE-03	OI-SRP7.2-ICE-06	OI-SRP7.9-ICE-05

Questions or requests for additional information related to the content and preparation of this response should be directed to Westinghouse. Please send copies of such questions or requests to the prospective applicants for combined licenses referencing the AP1000 Design Certification. A representative for each applicant is included on the cc: list of this letter.

Very truly yours,

Robert Sisk, Manager
Licensing and Customer Interface
Regulatory Affairs and Standardization

/Enclosure

1. Response to Proposed Open Item (Chapter 7)

DO63
NRO

cc:	D. Jaffe	-	U.S. NRC	1E
	E. McKenna	-	U.S. NRC	1E
	P. Kallan	-	U.S. NRC	1E
	S. Mitra	-	U.S. NRC	1E
	T. Spink	-	TVA	1E
	P. Hastings	-	Duke Power	1E
	R. Kitchen	-	Progress Energy	1E
	A. Monroe	-	SCANA	1E
	P. Jacobs	-	Florida Power & Light	1E
	C. Pierce	-	Southern Company	1E
	E. Schmiech	-	Westinghouse	1E
	G. Zinke	-	NuStart/Entergy	1E
	R. Grumbir	-	NuStart	1E
	B. Seelman	-	Westinghouse	1E

ENCLOSURE 1

AP1000 Response to Proposed Open Item (Chapter 7)

AP1000 TECHNICAL REPORT REVIEW

Response to Open Item (OI)

RAI Response Number: OI-SRP7.1-ICE-02
Revision: 0

Question:
In support of Revision 17 of the AP1000 DCD, the staff reviewed the following WEC TRs:

- APP-GW-GLR-071/WCAP-16675-P, Revision 2 (TR-89). This report describes how the PMS will function. Section 7.2.2, "Protection and Safety Monitoring System Description," and Section 7.9 of this supplement discuss this report.
- APP-GW-GLR-065/WCAP-16674-P, "AP1000 I&C Data Communication and Manual Control of Safety Systems and Components," Revision 1 (TR-88). This report provides critical design aspects of the communications methodology and various protocols when dealing with inter- and intra-division communications and safety-related-to-non-safety-related communications methods. The report also contains key information on the manual operation of the AP1000 safety systems. Sections 7.2.2; 7.5.3, "Network Gateway"; 7.9.3, "Communication between Safety and Nonsafety Systems"; and 7.9.4, "Nonsafety Communications," of this FSER supplement discuss APP-GW-GLR-065 in greater detail.
- APP-GW-GLN-022, "AP1000 Standard Combined License Technical Report DAS Platform Technology and Remote Indication Change," Revision 1 (TR-97), dated May 14, 2007. This report provides information associated with the location of DAS equipment, and it incorporates changes to allow a microprocessor-based or alternative technology to serve as the principal design of the DAS platform. Section 7.1.6, "Diversity and Defense in Depth Assessment," and Section 7.8 discuss APP-GW-GLN-022.
- APP-GW-GLR-017, Revision 0 (TR-42). This report summarizes WEC's proposed resolution of the 10 generic open items (GOIs) and 14 plant-specific action items (PSAIs) associated with the NRC review of the WEC Common Q platform. Section 7.2.3, "Common Qualified Platform Design and COL Action Items," contains more information on this document.
- APP-GW-GLR-024, "AP1000 Setpoint Calculations for Protective Functions," Revision 0 (TR-28). This report discusses the calculation of setpoints and setpoint methodology. Section 7.2.7, "Protection Systems Setpoint Methodology," contains additional information on setpoint methodology in AP1000 I&C systems.
- APP-GW-GLR-018, "Failure Modes and Effects Analysis and Software Hazards Analysis for AP1000 Protection System," Revision 0 (TR-43). This report summarizes the steps taken to perform the failure modes and effects analysis (FMEA) and software hazards analysis (SHA) and serves primarily as a pointer to the AP1000 FMEA and SHA reports.
- APP-GW-JJ-002, "FMEA of AP1000 Protection and Safety Monitoring System," Revision 2 (WCAP-16438-P). This report provides the postulated failure modes and effects the PMS will undergo as a result of the given failures.
- APP-GW-GLN-004, "Instrument and Control Design Change," Revision 0 (TR-39), incorporates signal and other name changes to the postaccident monitoring system (PAMS), which interfaces with the qualified data processing system (QDPS). In reviewing the submitted documents and Revision 17 of the AP1000 DCD, the staff

identified a newer revision of a TR referenced in Revision 17 but not provided for staff review. WEC must submit TR WCAP-16592-P, "Software Hazards Analysis of AP1000 Protection and Safety Monitoring System," Revision 1, to the NRC. **The NRC staff identified this as OI-SRP-7.1-ICE-02.**

Westinghouse Response:
Document WCAP-16592-P (APP-PMS-GER-001), Rev 1 "Software Hazards Analysis of AP1000 Protection and Safety Monitoring System" was submitted on the docket via letter DCP_NRC_002720 dated December 17, 2009. The report presents the Software Hazard Analysis (SHA) for the AP1000 Protection and Safety Monitoring System (PMS) and addresses the Combined Operating License (COL) item identified in APP-GW-GL-700, "AP1000 Design Control Document" (Reference 4) Section 7.2.3. It also provides the NRC with the version of the document referenced in the DCD Rev 17.

References:

1. WCAP-16592-P (APP-PMS-GER-001), Rev 1 "Software Hazards Analysis of AP1000 Protection and Safety Monitoring System"

Design Control Document (DCD) Revision:
None

PRA Revision:
None

Technical Report (TR) Revision:
1. WCAP-16592-P (APP-PMS-GER-001), Rev 1 "Software Hazards Analysis of AP1000 Protection and Safety Monitoring System"

AP1000 TECHNICAL REPORT REVIEW

Response to Open Item (OI)

RAI Response Number: OI-SRP7.1-ICE-03
Revision: 0

Question:

In Section 7.1.7, "References," of Revision 17 of the AP1000 DCD, WEC deleted several references from the certified reference section without sufficient basis. Specifically, Reference 11, "Acceptance for Referencing of Topical Report CENPD-396-P, 'Common Qualified Platform' and Appendices 1, 2, 3 and 4," Revision 1, contains information critical in assisting the staff in determining the acceptability of AP1000 I&C systems. In addition, although it is identified in the text of TR WCAP 16675-P, WEC makes no reference to TR WCAP 16674-P, Revision 1, in Section 7.1.7 of the AP1000 DCD or in the references for TR WCAP 16675-P. WEC should explain why the NRC should allow the removal of each of the specific references from Section 7.1.7 of the AP1000 DCD and why WEC did not include TR WCAP 16674-P in the reference section. **The NRC staff identified this as OI-SRP-7.1-ICE-03.**

Westinghouse Response:

Westinghouse deleted some of the references in an effort to remove redundant information. For example, the reference to "Acceptance for Referencing of Topical Report CENPD-396-P, 'Common Qualified Platform' and Appendices 1, 2, 3 and 4," was deleted because WCAP-16097-P-A contains the same Safety Evaluation Report and therefore WEC found it to be redundant. In regards to the WCAP references, WCAP-16675 (TR-89), which is referenced in the DCD, was revised and was submitted to the NRC in December 2009. This latest revision of WCAP-16675 contains a reference to WCAP-16674 (TR-88).

References:

1. WCAP-16674-P (TR-88), "AP1000 I&C Data Communication and Manual Control of Safety Systems and Components."
2. WCAP-16675-P (TR-89), "AP1000 Protection and Safety Monitoring System Architecture Technical Report"

Design Control Document (DCD) Revision: None

PRA Revision: None

Technical Report (TR) Revision:

1. WCAP-16675: WCAP-16674 will be added to the list of references.

AP1000 TECHNICAL REPORT REVIEW

Response to Open Item (OI)

RAI Response Number: OI-SRP7.2-ICE-04
Revision: 0

Question:

7.2.2.3.13 Integrated Logic Processor Technical Evaluation

The ILPs serve as the action-sequencing logic; they distribute the activate signal to the various CIMs. The staff found no portion of the Common Q topical report or other report that provided an analysis suitable to allow for a conclusion that the ILP is a highly reliable device within a safety system. Based on the design information in WCAP-16675-P, the ILP acts as an intradivisional interface device between the comparative logic device (e.g., LCL) and the SRNC, which forwards its output to the priority module (CIM). The ILP may use a design previously approved by the NRC (i.e., Common Q equipment). However, the staff has identified no design information within docketed material revealing this possibility. As the Common Q topical report did not previously approve the use of an ILP, WEC should describe, in the AP1000 DCD or one of the associated TRs, how the equipment meets regulatory requirements; specifically, IEEE Std. 603-1991 and the GDC 21-24. WEC should also identify the equipment used to develop the ILP. **The NRC staff identified this as OI-SRP-7.2-04.**

Westinghouse Response:

Westinghouse WCAP-16675 (TR-89), which was submitted on the docket by DCP_NRC_002726 dated December 30, 2009, explicitly states that the ILP is an AC160 controller that has been generically approved by the NRC for safety applications.

References:

1. WCAP-16675 (APP-GW-GLR-071), "AP1000 Protection and Safety Monitoring System Architecture Technical Report" (TR-89)

Design Control Document (DCD) Revision: None

PRA Revision: None

Technical Report (TR) Revision:

1. WCAP-16675 (APP-GW-GLR-071), "AP1000 Protection and Safety Monitoring System Architecture Technical Report" (TR-89)

AP1000 TECHNICAL REPORT REVIEW

Response to Open Item (OI)

RAI Response Number: OI-SRP7.2-ICE-06
Revision: 0

Question:
7.2.2.3.15 Safety-Related Remote Node Controller Technical Evaluation
The staff conducted an audit that dealt with the review of WEC Phase 1 and Phase 2 proprietary documents for the AP1000 PMS SLC on April 20–22, 2009, in Cranberry, PA (see audit report under ADAMS Accession No. ML091560352). During the demonstration of a "test" system, the staff learned of a new device that WEC would add to the PMS. WEC demonstrated the use of an SRNC that would serve as the interface device from the ILP to the CIM. Under previous revisions of TRs, no intermediary device existed between the ILP and the CIM. Although WEC discussed the device's function generically in WCAP-16675-P, it offered no discussion regarding how the SRNC meets the requirements of IEEE Std. 603-1991. The staff requires such additional information regarding the overall design quality, independence, and reliability of the SRNC before it can find the use of this device in the PMS acceptable. **The NRC staff identified this is as OI-SRP-7.2-06.**

Westinghouse Response:
As demonstrated by WEC in the April 2009 audit, the Safety Remote Node Controller (SRNC) is one of the CIM components. It serves as the interface device from the ILP to the CIM. The functionality of the SRNC is discussed in WCAP-16675-P. Communication with the PMS is accomplished with the SRNC assembly. The CIM and SRNC provide the control of the safety-related components through the PMS. This actuation path must be diverse from the path that is provided in the DAS.

WEC submitted WCAP-17179-P (APP-GW-GLR-143) Revision 0, "AP1000 Component Interface Module Technical Report" to the NRC via DCP_NRC_ 002725 dated December 30, 2009, which contains a more detailed description of how the SRNC meets the design, independence, and reliability to satisfy the requirements of IEEE Std. 603-1991.

References:

1. WCAP-17179-P (APP-GW-GLR-143) Revision 0, "AP1000 Component Interface Module Technical Report

Design Control Document (DCD) Revision: None

PRA Revision: None

Technical Report (TR) Revision: None

AP1000 TECHNICAL REPORT REVIEW

Response to Open Item (OI)

RAI Response Number: OI-SRP7.9-ICE-02
Revision: 0

Question:

Demonstrate how the design of the hardwired interfaces used to send analog and digital signal from the PMS to the PLS meet the independence requirements of IEEE Std. 603-1991 Clause 5.6.3, and GDC 24.

Section 5 of WCAP-16674 states that for Case A and Case B types of communication between the PMS and non-safety equipment, qualified isolation devices are used to provide communications independence between the PMS and the PLS. 10 CFR 50.55(a)(h) incorporates by reference IEEE Std. 603-1991, "Standards and Criteria for Safety System Design." IEEE Std. 603-1991, Clause 5.6.3 requires independence between safety and non-safety systems such that credible failures in and consequential actions by non-safety systems shall not prevent the safety system from accomplishing its intended safety function. In addition, Appendix A of 10 CFR 50, General Design Criterion (GDC) 24 requires the protection system to be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel which is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system. Demonstrate how the qualified isolation devices used in Case A and Case B provide communications independence between the PMS and the PLS to meet IEEE Std 603-1991, Clause 5.6.3, and GDC 24. Specifically, the staff requests the applicant provide specific design information to describe how communications independence is achieved (e.g. simple discrete digital signals).

Westinghouse Response:

The text describing Case A and Case B in WCAP-16674 (Reference 1) and WCAP-16675 (Reference 2) were changed to use the term "discrete digital signals" instead of "digital signals." Additionally, the references to IEEE 7.4.3.2 were eliminated from those cases. Both Westinghouse WCAP-16675 (TR-89) and WCAP-16674 (TR-88) were submitted on the docket by DCP_NRC_002726 dated December 30, 2009.

References:

1. WCAP-16674-P (TR-88), "AP1000 I&C Data Communication and Manual Control of Safety Systems and Components."
2. WCAP-16675-P (TR-89), "AP1000 Protection and Safety Monitoring System Architecture Technical Report."

AP1000 TECHNICAL REPORT REVIEW

Response to Open Item (OI)

Design Control Document (DCD) Revision: None

PRA Revision: None

Technical Report (TR) Revision:

The second and third paragraphs of Section 5.1.1 in WCAP-16674 (Reference 1) will be changed to read as follows:

> "The PMS also provides data to the PLS pertaining to analog and discrete digital signals calculated within the PMS (e.g., Over Temperature Delta Temperature Margin to Trip). These signals are classified as safety-related and are, therefore, isolated in the PMS cabinets before being sent to the PLS as individual hardwired analog or discrete digital signals. This type of interface is shown as Case B on Figure 5-1 and is identical to the type of interface in existing Westinghouse plants.
>
> "In both cases, qualified isolation devices are used. These devices provide electrical isolation between the systems (as required by IEEE 603-1991 {Reference 8.}) They also provide functional isolation by preventing the non-safety system from adversely affecting the safety function."

The second paragraph of Section 3.3.1 in WCAP-16675 (Reference 2) will be changed to read as follows:

> "Qualified isolation devices are used. These devices provide electrical isolation between the systems (as required by IEEE 603-1991 {Reference 7.}) They also provide functional isolation by preventing the non-safety system from adversely affecting the safety function."

The first and second paragraphs of Section 3.3.2 in WCAP-16675 (Reference 2) will be changed to read as follows:

> "The PMS also provides data to the PLS pertaining to analog and discrete digital signals calculated within the PMS (e.g., Over Temperature Delta Temperature Margin to Trip). These signals are classified as safety-related and are, therefore, isolated in the PMS cabinets before being sent to the PLS as individual hardwired analog or discrete digital signals. This type of interface is shown as Case B on Figure 3-1 and is identical to the type of interface in existing Westinghouse plants.
>
> "Qualified isolation devices are used. These devices provide electrical isolation between the systems (as required by IEEE 603-1991 {Reference 7.}) They also provide functional isolation by preventing the non-safety system from adversely affecting the safety function."

AP1000 TECHNICAL REPORT REVIEW

Response to Open Item (OI)

RAI Response Number: OI-SRP7.9-ICE-05
Revision: 0

Question:

Clarify whether any of the non-safety data links described in Section 3.2 of WCAP-16674 interfaces with the PMS.

Section 3.2 of WCAP-16674 provides a description of the Non-Safety Data Link Interfaces within the AP1000 I&C design. IEEE Std. 603-1991, Clause 5.6.3 requires independence between safety and non-safety systems such that credible failures in and consequential actions by non-safety systems shall not prevent the safety system from accomplishing its intended safety function. In addition, Appendix A of 10 CFR 50, General Design Criterion (GDC) 24 requires the protection system to be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel which is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system. The staff requests the applicant provide information to clarify whether any of these non-safety data link interfaces communicates with the safety system beyond the five cases of safety to non-safety system data communications specified in WCAP-16674. If such communications exist, demonstrate how electrical isolation, and communications and functional independence are provided as required by IEEE Std. 603-1991, Clauses 5.6.3, and GDC 24.

Westinghouse Response:

Text was added to WCAP-16674 (Reference 1) stating that the non-safety network and datalinks described in Section 3 of the WCAP do not directly communicate with the safety systems except as described in Section 5. Westinghouse WCAP-16674 (TR-88) was submitted on the docket by DCP_NRC_002726 dated December 30, 2009.

References:

1. WCAP-16674-P, "AP1000 I&C Data Communication and Manual Control of Safety Systems and Components."

Design Control Document (DCD) Revision: None

PRA Revision: None

AP1000 TECHNICAL REPORT REVIEW

Response to Open Item (OI)

Technical Report (TR) Revision:

The first paragraph of Section 3 in WCAP-16674 (Reference 1) will be changed to read as follows:

> "Non-safety communication consists primarily of the non-safety communication network and the non-safety datalink interfaces. These interfaces do not directly communicate with the safety systems, except as described in Section 5."